OrangeHRM Enterprise Application

Middleware Installation Guide - Advanced

OrangeHRM 7.4 and Above
Version 1.1

All rights reserved. Published in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical photocopying, and recording or likewise. For more information regarding permissions please contact us on info@orangehrm.com

Document History

Release Date	Version No.	Author(s)	Description	Recommended by	Approved by
February 10, 2022	1.0	ISO	Initial Release	Tech Ops	HOD
April 17, 2024	1.1	ISO	Moved RabbitMQ to a separate guide	TechOps	HOD

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

Table of Contents

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

1. Introduction

OrangeHRM is a web-based HRMS application which supports Apache, MariaDB, and PHP(AMP). This document describes the steps to be taken in order to prepare the middleware layer prior to installing the OrangeHRM Application.

Some of the configuration details referenced in this guide may vary depending on the specific application requirements and infrastructure resource availability. OrangeHRM Support Services team will assist you with such changes.

This document encompasses four major segments:

OrangeHRM Middleware Quick Installation - Manual

Please refer to the following sections in the document and follow the respective steps

1. Software Platform Preparation - Mandatory Steps
2. Apache virtual host configuration

OrangeHRM Middleware Installation With Platform Security Settings

Please refer to the following sections in the document and follow the respective steps

1. Software Platform Preparation - Mandatory Steps
2. Apache virtual host configuration
3. Software Platform Preparation - Security Enhancements

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

1.1 Required OrangeHRM Instances

Two instances of OrangeHRM are required for an onsite installation.

1. **Production Instance** - This is the live system which will be used by all the end-users and admins.

2. **Pre-Production Instance** - This is the instance that mimics the Production instance and is used for testing prior to any new deployments being applied to the Production instance. Once testing successfully concludes on the Pre-Production instance, the new build/patch would then be applied to the Production instance.

It is highly recommended to have two servers/VMs for the two instances. Both servers should be exactly the same in terms of hardware and software configuration. Please refer to the Hardware Requirements section in ***OrangeHRM-HW-SW-Requirements-Guide*** for details of the required hardware specifications.

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

2. Software Platform Installation - Mandatory

2.1 Software Dependencies Related Tasks

Commands referenced are prepared based on Ubuntu 20.04. Errors may be encountered due to possible conflicts between dnf packages and dependency-related issues. In such circumstances, cases will need to be analyzed individually and resolved accordingly.

IMPORTANT

- Make sure SSL certificates are prepared correctly
    - Please refer to the steps outlined in Appendix A - Create SSL certificates with openssl
- Prior to the installation
    - Update packages to the latest versions and restart the server (or virtual machine).

```
orangehrm@workspace:~ sudo apt update -y
orangehrm@workspace:~ sudo apt upgrade -y
```

- Commands are prepared based on Ubuntu 20.04

Install the following utility tools:

```
orangehrm@workspace:~ sudo apt install vim wget unzip curl
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

2.1.1 Install Apache

1. Apache Installation

```
orangehrm@workspace:~ sudo apt update
orangehrm@workspace:~ sudo apt install -y apache2
```

2. Apache preliminary configurations

```
orangehrm@workspace:~ sudo update-rc.d apache2 defaults
orangehrm@workspace:~ sudo service apache2 start
```

3. Enable Apache modules

```
orangehrm@workspace:~ sudo a2enmod ssl
orangehrm@workspace:~ sudo a2enmod headers
orangehrm@workspace:~ sudo a2enmod rewrite
orangehrm@workspace:~ sudo a2enmod expires
orangehrm@workspace:~ sudo systemctl restart apache2
```

2.1.2 Install PHP

1. Install prerequisites

```
orangehrm@workspace:~ sudo apt install -y libaio1 libfreetype6-dev
libmemcached-dev libssh2-1-dev libmcrypt-dev pkg-config libbson-1.0-0
libmongoc-1.0-0 zlib1g-dev
```

2. Install PHP

```
orangehrm@workspace:~ sudo apt install -y php php-pear php-dev php-tidy
php-bcmath php-bz2 php-curl php-gd php-gmp php-ldap php-mbstring php-soap
php-sqlite3 php-imap php-mysql php-zip libapache2-mod-php7.4
```

3. Install Third Party PHP packages

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

```
## please keep the default answers for all the questions asked during the
installation
orangehrm@workspace:~ sudo pecl install ssh2-1.3.1 igbinary-3.2.4
memcached-3.1.5 apcu-5.1.20 mcrypt-1.0.4
```

4. Execute the following commands

a. Enable APCU Extension

```
orangehrm@workspace:~ echo "extension=apcu.so" | sudo tee
/etc/php/7.4/mods-available/apcu.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/apcu.ini
/etc/php/7.4/cli/conf.d/apcu.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/apcu.ini
/etc/php/7.4/apache2/conf.d/apcu.ini
```

b. Enable Mcrypt Extension

```
orangehrm@workspace:~ echo "extension=mcrypt.so" | sudo tee
/etc/php/7.4/mods-available/mcrypt.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/mcrypt.ini
/etc/php/7.4/cli/conf.d/mcrypt.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/mcrypt.ini
/etc/php/7.4/apache2/conf.d/mcrypt.ini
```

c. Enable SSH2 Extension

```
orangehrm@workspace:~ echo "extension=ssh2.so" | sudo tee
/etc/php/7.4/mods-available/ssh2.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/ssh2.ini
/etc/php/7.4/cli/conf.d/ssh2.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/ssh2.ini
/etc/php/7.4/apache2/conf.d/ssh2.ini
```

d. Enable IGBINARY Extension

```
orangehrm@workspace:~ echo "extension=igbinary.so" | sudo tee
/etc/php/7.4/mods-available/igbinary.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/igbinary.ini
/etc/php/7.4/cli/conf.d/igbinary.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/igbinary.ini
/etc/php/7.4/apache2/conf.d/igbinary.ini
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

e. Enable MEMCACHED Extension

```
orangehrm@workspace:~ echo "extension=memcached.so" | sudo tee
/etc/php/7.4/mods-available/memcached.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/memcached.ini
/etc/php/7.4/cli/conf.d/memcached.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.1/mods-available/memcached.ini
/etc/php/7.4/apache2/conf.d/memcached.ini
```

- After the PHP installation is completed, please make sure the system has the following list of PHP modules (run "***php -m***")
    - apcu,bcmath,bz2,calendar,Core,ctype,curl,date,dom,exif,fileinfo,filter,ftp,gd,gettext, gmp, hash, iconv, igbinary, imap, ionCube Loader (refer to the section 2.1.2.2) , json,ldap,libxml,mbstring,mcrypt,memcached,mysqli,mysqlnd,openssl,pcntl,pcre, PDO,pdo_mysql,pdo_sqlite,Phar,posix,readline,Reflection,session,shmop,SimpleXML,soap,sockets,SPL,sqlite3,ssh2,standard,sysvmsg,sysvsem,sysvshm,tidy,tokenizer,xml,xmlreader,xmlwriter,xsl,zip,zlib

2.1.2.1 Recommended php.ini Settings

1. Open both php.ini files (apache2 and cli) and add / modify the following recommended values. (ensure the original configuration file is backed up prior to editing)

```
orangehrm@workspace:~ sudo vim /etc/php/7.4/apache2/php.ini
orangehrm@workspace:~ sudo vim /etc/php/7.4/cli/php.ini
```

```
short_open_tag = off
error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT & ~E_NOTICE
upload_max_filesize = 50M
memory_limit = 2048M
max_execution_time = 300
max_input_vars = 1500
expose_php = off
date.timezone = <as per client timezone: eg: asia/colombo>
enable_dl = off
allow_url_fopen = off
allow_url_include = off
display_errors = off
post_max_size = 50M
session.cookie_secure = 1
upload_tmp_dir = /tmp
precision = 14
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

2. After changing *php.ini* settings, please make sure to restart the Apache service

```
orangehrm@workspace:~ sudo apache2ctl -t
orangehrm@workspace:~ sudo service apache2 restart
```

2.1.2.2 ionCube Loader

OrangeHRM uses IonCube for encryption and licensing. To use encrypted code, a php extension called "Ioncube Loader" must be installed on your web server.
Follow the steps outlined below to install ionCube:

1. Download ionCube module

```
orangehrm@workspace:~ wget
https://downloads.ioncube.com/loader_downloads/ioncube_loaders_lin_x86-64.zip
```

NOTE

If the download link is not working please go to https://www.ioncube.com/loaders.php and download linux 64 bit supported ioncube encoder

2. Unzip the downloaded file

```
orangehrm@workspace:~ unzip ioncube_loaders_lin_x86-64.zip
```

3. Copy php7.4 supported ionCube module into php extension directory

    a. How to find an extension directory

```
orangehrm@workspace:~ php -i | grep ^extension_dir
```

```
#output should be as below
#extension directory path and name may deviate from the value given #below
extension_dir => /usr/lib/php/20190902 => /usr/lib/php/20190902
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

b. Copy ionCube module

```
orangehrm@workspace:~ sudo cp <ioncube extracted
dir>/ioncube_loader_lin_7.4.so <extension directory path>/ioncube.so
```

c. Verify the existence of the module

```
orangehrm@workspace:~ ls -l <extension directory path>/ioncube.so
```

4. Enable ionCube module

```
orangehrm@workspace:~ echo "zend_extension=ioncube.so" | sudo tee
/etc/php/7.4/mods-available/00-ioncube.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/00-ioncube.ini
/etc/php/7.4/cli/conf.d/00-ioncube.ini
orangehrm@workspace:~ sudo ln -s /etc/php/7.4/mods-available/00-ioncube.ini
/etc/php/7.4/apache2/conf.d/00-ioncube.ini
```

2.1.3 Install MariaDB

1. Installation

```
orangehrm@workspace:~ cd ~ && sudo curl -LsS -O
https://downloads.mariadb.com/MariaDB/mariadb_repo_setup
orangehrm@workspace:~ sudo bash mariadb_repo_setup
--mariadb-server-version=10.4.22
orangehrm@workspace:~ sudo apt -y install mariadb-server mariadb-client
```

2. Execute the following binary and provide the relevant details to secure the MariaDB server

```
orangehrm@workspace:~ sudo service mariadb restart
orangehrm@workspace:~ sudo mysql_secure_installation
```

Upon execution of the **mysql_secure_installation** command, you will be asked a series of general questions. You can answer them based on your preferences. (We have included suggested inputs below)

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

```
Enter current password for root (enter for none): press enter

Switch to unix socket authentication [Y/n] n

Change the root password? [Y/n] Y
(We recommend creating a strong password)
New password: <new password>
Re-enter new password: <confirm new password>

Remove anonymous users? [Y/n] Y

Disallow root login remotely? [Y/n] Y

Remove test database and access to it? [Y/n] Y

Reload privileged tables now? [Y/n] Y
```

3. Enable MariaDB to start on reboot

```
orangehrm@workspace:~ sudo systemctl enable mariadb
orangehrm@workspace:~ sudo service mariadb restart
```

4. Remove the temp bash scripts

```
orangehrm@workspace:~ sudo rm -f ~/mariadb_repo_setup
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

2.1.3.1 Recommended MariaDB Configurations

1. Recommended configurations are mentioned below. Edit my.cnf file and add/change the following values under the [mysqld] section. (ensure the original configuration file is backed up prior to editing)

```
orangehrm@workspace:~ sudo vim /etc/mysql/my.cnf

#add following configurations under [mysqld]

innodb_buffer_pool_size         = 2G
innodb_log_file_size            = 1G
innodb_lock_wait_timeout        = 30
innodb_log_buffer_size          = 8M
sql_mode                        = ""
max_allowed_packet              = 64M
connect_timeout                 = 60
delayed_insert_timeout          = 300
interactive_timeout             = 600
net_read_timeout                = 30
net_write_timeout               = 60
slave_net_timeout               = 600
wait_timeout                    = 600
event-scheduler                 = on
innodb_flush_log_at_trx_commit  = 1
skip-name-resolve
skip-host-cache
skip-name-resolve
```

2. Once changed, restart the MariaDB server

```
#restart mariadb service
orangehrm@workspace:~ sudo service mariadb restart
```

3. You can verify whether a mysql event scheduler is enabled or not by executing the following query in MariaDB

```
MariaDB [DBName]> SELECT @@event_scheduler;
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

2.1.4 Other Server Dependencies

After completing the middleware configurations detailed above, please install the following server dependencies:

```
orangehrm@workspace:~ sudo apt install fonts-urw-base35 poppler-utils
libreoffice-draw libreoffice-writer libssl-dev libmagickwand-dev
imagemagick -y
```

2.1.5 Install and Configure RabbitMQ [Optional]

RabbitMQ service is required only if the integrations are used with the application.

Please refer: RabbitMQ Installation & Configuration Guide

NOTE:

OrangeHRM support will promptly notify you if RabbitMQ installation is needed. If required, please refer to the RabbitMQ Installation Guide.

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

2.1.6 Post middleware installation verification

In order to verify the middleware installation, we have developed an automated script. Please follow the steps given below to download and verify your installation status.

1. Download verification script

```
orangehrm@workspace:~ wget https://alge.orangehrm.com/downloads/SeAT
```

2. Execute the following command (this is an example command and you can swap values according to your environment)

```
orangehrm@workspace:~ sudo php SeAT \
--db-host <db host>\
--db-port <db port> \
--db-root-user <root user>\
--db-root-password <password> \
--output-file <output file path>\
--output-format html
```

3. For more information on the script, execute the following command:

```
orangehrm@workspace:~ php SeAT --help
```

4. Then open up the output HTML file via your browser, analyze the results and make changes if needed.

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

3. Apache virtual host configuration

This section explains how apache virtual host configurations should be set prior to installing the OrangeHRM Application.

1. Create a directory in web root to host the OrangeHRM application

```
orangehrm@workspace:~ sudo mkdir /var/www/html/orangehrm
```

2. Modifying Apache configuration of the Web server allows support for .htaccess files.

    a. Open apache2.conf

```
orangehrm@workspace:~ sudo vim /etc/apache2/apache2.conf
```

    b. Append the following content into the apache2.conf file, save and exit

```
<Directory /var/www/html/orangehrm/symfony/web>
    Options FollowSymLinks
    AllowOverride All
    Order allow,deny
    allow from all
</Directory>
```

Above is an example. You may need to alter as per your environment details.

3. Configure the Apache Virtual Host for OrangeHRM with SSL connections. (*Below is an example. You may need to alter as per your environment details*)

    a. Create a new file on /etc/apache2/sites-available/orangehrm.conf

```
orangehrm@workspace:~ sudo vim /etc/apache2/sites-available/orangehrm.conf
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

b. Add the following content:

```
<VirtualHost *:443>
  ServerAdmin webmaster@orangehrm.com
  DocumentRoot /var/www/html/orangehrm/symfony/web
  ServerName <web site domain>
  SSLCertificateFile <public key certificate path>
  SSLCertificateKeyFile <private key certificate path>
  SSLCACertificateFile <CA certificate path>
  SSLEngine on
  RequestHeader unset Client-IP
  RequestHeader append Client-IP "%{REMOTE_ADDR}s"
  Header edit Set-Cookie ^(.*)$ $1;SameSite=none
</VirtualHost>
```

c. Enable the site and reload the Apache service.

```
orangehrm@workspace:~ sudo a2ensite orangehrm
orangehrm@workspace:~ sudo apache2ctl -t
orangehrm@workspace:~ sudo service apache2 reload
```

IMPORTANT

Installing the OrangeHRM application is the responsibility of the OrangeHRM Support Services team. Please contact your OrangeHRM Sales representative or Account Manager for assistance after completing the Middleware installation and Apache setup, or if you have any issues during the platform preparation process.

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

4. Server Security Hardening - Security Enhancements

The following guidelines must be adhered to in order to reduce the risk of an external attack. These recommendations prevent outsiders from gaining access to the system or overloading servers making them vulnerable to malicious and harmful attacks. However, clients can use any other preferred tools (including commercial tools if necessary) to conduct the assessments listed below.

4.1 General Recommendations

4.1.1 Disable Directory Listing and Special File Access

The “symfony” framework used in OrangeHRM itself supports the protection of the business logic from unauthorized access. This is accomplished by making all the directories inaccessible by URL if the document root of the application is set to symfony/web directory. But in order to ensure external parties cannot access the files outside the web directory, we have to make sure the following configurations are added to the server.

Add the following tag to the **/etc/apache2/apache2.conf** and then reload the Apache server

```
<Directory "give the path to OrangeHRM root directory">
    Options -Indexes
</Directory>
```

If you need to reproduce the above mentioned security risk, remove the ***minus(-)*** from the parameter ***-Indexes*** in apache2.conf. This will enable directory listing and you can navigate through the file structure with a browser.

Append the following best practice recommendations to the apache2.conf file:

```
# Allowing .htaccess
<Directory _ORANGEHRM_ROOT_DIR_>
  AllowOverride All
</Directory>

# Limiting .svn listing
<DirectoryMatch .*\.svn/.*>
   Order allow,deny
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

```
   Deny From All
</DirectoryMatch>

# Restricting .YML files
<Files ~ "\.yml$">
 Order allow,deny
 Deny from all
</Files>

DirectoryIndex index.html index.php
TraceEnable Off

LogFormat "%h %l %u %t \"%m %U\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%m %U\" %>s %b" common
```

```
# You need to enable mod_logio.c to use %I and %O
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%m %U\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I
%O" combinedio
</IfModule>
```

After defining the logs please make sure to add log rotation for your apache access and error logs

4.1.2 Block Unnecessary Ports

Use iptables/firewalld to enforce the firewall security on the server. OrangeHRM recommends keeping only the following ports open as a default list, however, depending on the clients' requirements, it can be determined what other legitimate ports may need to be opened.

In-Bound	Outbound
HTTP/HTTPS - 80/443	**HTTP/HTTPS** - 80/443
SSH - 22 or any other custom port if exists	**SMTP** - 587 or 465 (Decide based on the application mail configuration)

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

ICMP - (If required 3rd party hosting providers and/or monitoring tools. Allow only to specific IPs)	**ICMP** - (If required 3rd party hosting providers and/or monitoring tools. Allow only to specific IPs)
	SFTP - 22 or any other custom port if exists
	DNS - Default port 53 (UDP)
	LDAP/LDAPS - 636 or 389 (Decide based on the LDAP protocol)
	NTP - Default port 123 (UDP)

4.1.3 Stop Unnecessary Applications

Stop any services that are already running and are not required and switch them off from systemctl to remove them from the startup services list
You can use the following command to view the list of services available on the server.

```
orangehrm@workspace:~ sudo systemctl list-units
```

4.1.4 Security - Patch Updates

This section will explain how to automate security updates in installed packages. [Only the packages installed through repositories will be affected. Any package/ binary or any module which was installed manually, will have to be patched manually]

1. Install cron-apt

```
orangehrm@workspace:~ sudo apt install cron-apt
```

2. The configuration for cron-apt resides in /etc/cron-apt/config -- in terms of how often the script runs, this depends on cron so you can find it in /etc/cron.d/cron-apt.

   One popular configuration change is to add the following line to /etc/cron-apt/config

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

```
# Configuration for cron-apt. For further information about the possible
# configuration settings see /usr/share/doc/cron-apt/README.gz.

MAILON="always"
MAILTO="sysadmin@example.com"
```

This will make sure an email is always sent when the update runs, rather than only when an error occurs.

4.2 Security - Access Control Related Tasks

4.2.1 Restrict SSH 'root' Access

DO NOT grant ssh access to root/regular users unless it is requested.

4.2.2 Configure SSH ACL

Restrict SSH access to production servers to only support engineers/system administrators/DBAs using SSH ACL.

4.2.3 Configure User Groups

Group 1 : Application Maintenance team (OrangeHRM) should have the following:

1. Privileges to create, read, delete and update to the OrangeHRM code directory
2. Stop, Start, Reload, Config test Apache and MariaDB services
3. Edit MariaDB, Apache and PHP configuration
4. Execute mysqldump command with routines option

4.2.4 Restrict FTP

FTP users should be created as non privileged users. Disable the transfer of files from a production server using FTP. Alternatively, use SFTP services.

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

4.2.5 Enable security headers for Apache

a. Content Security policy is another Apache header which needs to be handled at the server level (add the policy as per the client's requirements. Not a mandatory requirement for OrangeHRM app installation)

b. Following header (HPKP) is not required for the OHRM application to function properly. However, it is recommended to enhance infrastructure security.
   i. Click on this link to configure.

4.2.6 Enabling LDAPS

If you are planning to setup an LDAPS connection you need to have the CA certificate of the LDAP Instance and perform the following steps. This section considers that you have an Active Directory Based LDAP implementation.

1. If the certificate is available please proceed to the Linux-based client section below

2. Alternatively, to enable this for the windows AD server, please follow the steps below:

   - Click Start -> Click on administrative tools -> issued certificates
   - Right-click on the root certificate chain - > click properties
   - General Tab -> Select the required CA cert -> view certificate
   - Select details tab
   - Click on "*Copy to file*" -> Click Next -> Select "*Base-64 encoded X.509*" -> click on Next
   - Provide a filename and save

Linux Based Client

- Then upload the CA cert [which you have acquired from the step above] into the respective Test server.
  - Location of the certificate : /etc/openldap/certs
  - Create a symlink for the certificate. Make sure the symlink name adheres to the following format
    - <CA Hash value>.0
    - CA Hash value can be generated using the following command
      - openssl x509 -noout -hash -in <ca cert file>

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

- Edit /etc/openldap/ldap.conf and add the following snippet
    - TLS_CACERTDIR /etc/openldap/cacerts
    - If you encounter the following line in the ldap.conf comment it out
        - #TLS_REQCERT never

4.3 Security - Data Access Related Tasks

4.3.1 Define sudo Aliases Permissions

Define sudo aliases and permissions to execute for the user groups, according to organizational policies.

4.3.2 Restrict Execution Permissions for Selected Linux Commands

Remove execute permissions from regular users for the following Linux commands:

- cp (except from and to within home directory)
- rm
- mv (except from and to within home directory)
- mysqldump
- mtools
- ftp
- sftp
- scp

4.3.3 Disable Telnet (If Enabled)

1. SSH into the server and login as root.

2. At the shell command prompt type the following command and press Enter.

```
orangehrm@workspace:~ sudo systemctl stop inetd
orangehrm@workspace:~ sudo systemctl disable inetd
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

4.4 Security - Audit Related Tasks

4.4.1 Setup a Preferred Audit Tool (optional)

I.e MariaDB audit plugin
https://mariadb.com/kb/en/library/mariadb-audit-plugin/

Also, we would recommend configuring an Intrusion Detection System such as PHPIDS which will add an additional layer of security.

4.4.2 Post Security Scanning

This section references the set of tools and services which help to identify improper security configurations and vulnerabilities which may exist in the server.

- Lynys - Host based Scanning tool
  This tool will detect improper middleware and OS level configurations in the host.
    - Tool is available in apt repositories. If this is not available in the host, please download it as follows:

```
orangehrm@workspace:~ wget -O -
https://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key
add -
orangehrm@workspace:~ echo "deb
https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee
/etc/apt/sources.list.d/cisofy-lynis.list
orangehrm@workspace:~ sudo apt update
orangehrm@workspace:~ sudo apt install lynis -y
```

    - Then execute the following command to run the system audit

```
orangehrm@workspace:~ sudo lynis audit system
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

- Qualys web security tool
  This tool will evaluate the SSL configuration of the server and provide recommendations upon results.
    - This is an online tool. Refer to the URL below
        - https://www.ssllabs.com/ssltest/
    - Provide the URL of your instance and let the tool scan the configuration
    - Strive to achieve the A+ Grade by applying the amendments recommended by the tool

NOTE

None of the above settings are mandatory for OrangeHRM applications to be deployed. However, these configurations are needed in order to enhance the security of the deployment environment.

4.5 Service Monitoring

4.5.1 Setup a Preferred Monitoring Tool

We recommend adding the OrangeHRM deployed server to an infrastructure monitoring tool such as Datadog, Zenoss or New Relic etc.

- New Relic - https://newrelic.com/
- Zenoss - https://www.zenoss.com/

If the servers are running on VMWare or Hyper-V or any other similar environment, the monitoring of servers (host machine) should also be enabled.

We would recommend monitoring the following parameters and configuring alerts to be triggered if the parameters are exceeded based on predefined threshold levels.

- CPU
- Memory
- Disk Usage
- Load Average
- MySQL Connections
- Network interface errors/Utilization

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

4.6 Configure NGINX Reverse Proxy [optional]

Go through the following steps to set up Nginx:

1. Stop existing Apache service (if the service is running)

```
orangehrm@workspace:~ sudo service apache2 stop
```

2. Install nginx

```
orangehrm@workspace:~ sudo apt install nginx && sudo update-rc.d nginx
defaults
```

3. Create nginx proxy

```
orangehrm@workspace:~ sudo touch /etc/nginx/sites-available/orangehrm.conf
```

4. Copy the following example configuration file and replace its place holders with required values as appropriate

```
server {
    listen 443 ssl;
    server_name "<domain name>";
    ssl_certificate           <Absolute path of public key file>;
    ssl_certificate_key       <Absolute path of private key file>;

    location / {

        limit_except GET POST PUT HEAD DELETE PATCH OPTIONS {
             deny   all;
        }

        proxy_pass https://<localhost or local IP>:<apache2 port>;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header Client-IP $remote_addr;
    }
}
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

5. Run the following command to enable the site

```
orangehrm@workspace:~ sudo ln -s /etc/nginx/sites-available/orangehrm.conf
/etc/nginx/sites-enabled/orangehrm.conf
```

6. Make sure the existing default http (Port 80) site configuration is disabled

```
orangehrm@workspace:~ sudo rm -f /etc/nginx/sites-enabled/default
```

7. Add the following section towards the end of the orangehrm.conf file if the client is not using HTTP protocol and only uses HTTPS traffic. This modification will direct all the HTTP web traffic that comes through port 80 into HTTPS.

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        server_name _;
        return 301 https://$host$request_uri;
}
```

8. Modify the following configurations into the /etc/nginx/nginx.conf file

```
keepalive_timeout 60
gzip on
```

9. Start nginx

```
orangehrm@workspace:~ sudo service nginx start
```

10. Update Apache listening port (ensure the original configuration file is backed up prior to editing)

```
orangehrm@workspace:~ sudo vim /etc/apache2/ports.conf
```

    a. Comment the “Listen 80” line and change the current listening port of 443 to 8080 (if 8080 is unavailable change the port number accordingly).

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

```
# /etc/apache2/sites-enabled/000-default.conf

#Listen 80

<IfModule ssl_module>
      Listen 8080
</IfModule>

<IfModule mod_gnutls.c>
      Listen 8080
</IfModule>
```

b. Go to the OrangeHRM applications vhost file (/etc/apache2/sites-available/orangehrm.conf) and change the listen port to 8080

```
<VirtualHost *:8080>
  ServerAdmin webmaster@orangehrm.com
  DocumentRoot _ORANGEHRM_ROOT_DIR_/symfony/web
  ServerName <web site domain>
  SSLCertificateFile <public key certificate path>
  SSLCertificateKeyFile <key certificate path>
  SSLCACertificateFile <CA certificate path>
  SSLEngine on
  RequestHeader unset Client-IP
  RequestHeader append Client-IP "%{REMOTE_ADDR}s"
</VirtualHost>
```

c. Start the Apache service

```
orangehrm@workspace:~ sudo service apache2 start
```

11. Go to nginx proxy file (/etc/nginx/sites-available/orangehrm.conf) and change proxy port to 8080

```
proxy_pass https://localhost:8080;
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

NOTE

If nginx is used as a reverse proxy, make sure that you remove the ***Client-IP HTTP header*** from the Apache level, if it is configured in the apache level.

4.7 Data Backups

We recommend you keep regular server backups. The preferred retention period is 2 weeks.
If you can have file-level backups and MariaDB/MySQL backups separately, this is preferable as it will be more convenient for data recovery purposes.

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

Appendix

Appendix A

Create SSL certificates with openssl

This section describes how to create a private key and generate a certificate signing request using openssl.

A.1 Create a certificate signing request (CSR)

SAN (subject alternative name) name must be referenced in the CSR. Create a file called **san.cnf** and add the following content. Replace the content according to the organization's requirements.

```
[ req ]
default_bits       = 2048
distinguished_name = req_distinguished_name
req_extensions     = req_ext
prompt = no
[ req_distinguished_name ]
countryName                = <COUNTRY_NAME>
stateOrProvinceName        = <STATE_OR_PROVINCE_NAME>
localityName               = <LOCALITY_NAME>
organizationName           = <ORGANIZATION_NAME>
commonName                 = <COMMON_NAME>
[ req_ext ]
subjectAltName = @alt_names
[alt_names]
DNS.1   = <DNS_ONE>
DNS.2   = <DNS_TWO>
DNS.3   = <DNS_THREE>
```

- <COUNTRY_NAME> = Country name.(two letter code - US, UK, etc)
- <STATE_OR_PROVINCE_NAME> = State or Province Name (full name)
- <LOCALITY_NAME> = Locality Name (eg, city)
- <ORGANIZATION_NAME> = Organization Name (eg, company)
- <COMMON_NAME> = Common Name (e.g. server FQDN or YOUR name)

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

Complete the **alt_name** section with your additional DNS names. If you only have one DNS name, then remove the DNS.2 and DNS.3 records.

- Run the following command to generate the private key and CSR (Certificate Signing Request).

```
orangehrm@workspace:~ openssl req -out <EXAMPLE.COM>.csr -newkey rsa:2048
-nodes -keyout <EXAMPLE.COM>.key -config san.cnf
```

- Use the command below to generate the CSR if you already have a private key.

```
orangehrm@workspace:~ openssl req -new -out <EXAMPLE.COM>.csr -key
<EXAMPLE.COM>.key -config san.cnf
```

- You can verify your CSR by checking that the CSR contains the SAN, which you specified in the san.cnf file.

```
orangehrm@workspace:~ openssl req -noout -text -in <EXAMPLE.COM>.csr | grep
DNS
```

A.2 Submit the CSR to a Certificate Authority

- Certificates should be signed by a trusted certificate authority.
- You should submit the generated CSR to your certificate authority and get the signed certificate.
- Make sure to export the signed certificate in base-64 format. This will be your public key.

A.3 Verify the certificates

- Private key and public key should be compatible with each other. Use the following command to verify the compatibility. If outputs from each command are identical then keys are compatible.

```
orangehrm@workspace:~ openssl x509 -noout -modulus -in <public key> |
openssl md5
orangehrm@workspace:~ openssl x509 -noout -modulus -in <private key> |
openssl md5
```

Copyright © OrangeHRM Inc. 2024. All Rights Reserved

- Verify the subject alternative name and common name is compatible with the application's domain name. Use the following command to verify the compatibility.
    - For the Subject alternative name
      If the output is received with DNS records which match the application's domain name then SSL certificate's subject alternative name should be compatible.

```
orangehrm@workspace:~ openssl x509 -text -noout -in <public key> | grep DNS
```

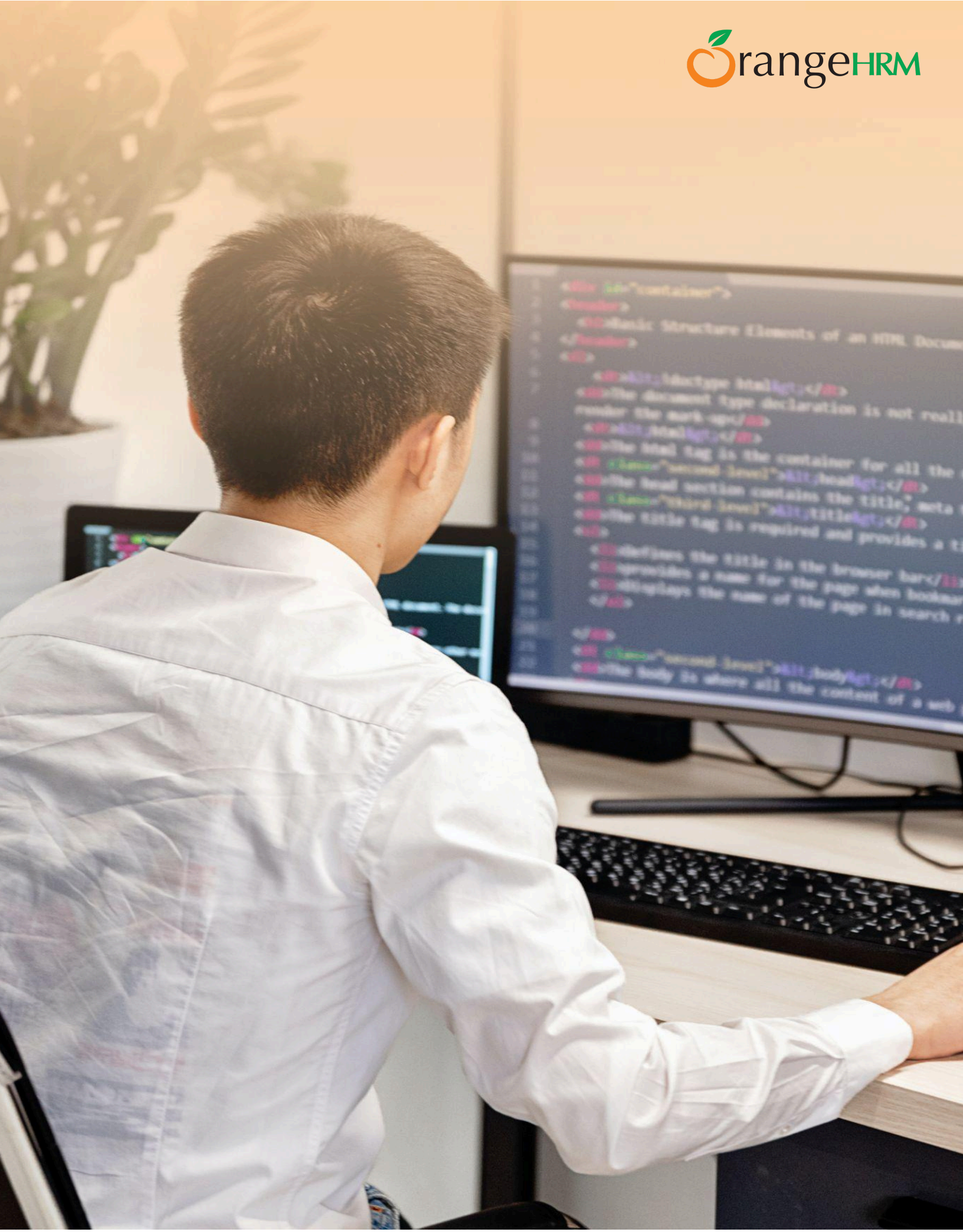
    - For the common name
      If the CN value of the output is compatible with the application's domain name then SSL certificate's common name should be compatible.

```
orangehrm@workspace:~ openssl x509 -noout -subject -in <public key>
```

NOTE

- If your certificate authority (CA) is an intermediate certificate authority, then make sure to create a single CA certificate including the complete certificate chain.
- Intermediate CA certificates should be arranged in the correct order. Root CA certificate should be added to the bottom.

Copyright © OrangeHRM Inc. 2024. All Rights Reserved


OrangeHRM